

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Криптографія
Лабораторна робота №3 (варіант 6)
Криптоаналіз афінної біграмної підстановки

Виконали:
студентки 3 курсу ФТІ
групи ФБ-93
Шрейдер Марія
Жембровська Олена

Перевірила:
Селюх П.В.

Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.
2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).
3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.
5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

В ході роботи ми йшли за пунктами з «порядку виконання роботи».

Помітили, що в алфавіті, яким шифрувався тест були переставлені місцями букви «ы» та «ь».

Найчастіші біграми шифртексту

['ще', 'хе', 'чв', 'ле', 'цв']

Розпізнавач російської мови

Був обраний ентропійний критерій відбору змістовного тексту.

Для розшифрованих текстів по кожному зі знайдених ключів рахується ентропія тексту без перетинів та порівнюється зі значеннями, які були знайдені в першій лабораторній. Це приблизно від 4.4 до 4.5.

Повертається ключ, за яким ентропія розшифрованого тексту входить в даний проміжок.

Зашифрованный текст

ывлеюгзебшпещхщуйэвиывиюфгувхцубхщюнюжлепэшфмиьхдошбуднзегдшебоцвшуюгьпцвэ
шувкмзеиэбчиюндхшюасдбмонхегштгдэшжезьшемвошфысьмайыегыййййэшжеаекидшщекжгь
деьцонгочвнюиюжвжудеьбюгьщесфвшвокуэйэяшкщьюгочвнюлмшужеейцурпцвдэяхщаюьдеу
эвющэвдияйтвепцвчвлеюйщецыаешвэеяиктехщаэацизибвкмрйжуажййдекуштепэшфмздсу
гьвоцвайкзфштшхдуюиьйнюгдхацовойэрашеюияцияимюжцввджвяцэввлломоодмхщуйэм
юззопюзкнэщегбдсефвьхбжщенюцатщввэиегтеаехохтюйлдицзьхдшщюяьзщюоцвлеюосдлу
элзащавызийферддйомюиаыьепжмнюбжщцаешэзойтзэвзщупмюжьощаощвыжееююзьдеаей
юшдоездюйбпгьвиюэколпшхмоихсшфеэмлеотзомшйвхцывбжжебахизьщхйэашжеттфележебд
фюфпнюфмшуиэжяппшдгдщесдцжцвхеюцхеднвжееютбзийысддемилпмюзахшнюллоюэпподй
шяюьхщужуиуцтабззлзыйопнбояшпиэщиамленйхдбднвншлврпшилмиьадшахушайыэффппмю
цдсззезщадцьцихжшущфгбиэихеныжпбоцднесдегмаушйыктгдйктийнвмоктздгидатаомтшл
вхеййрдияцшущюывмтшзюашнэьгозавюрдвджгмпиеэщеиэивдодзехатщйыэшзэшзунзщхеюи
зчсдэайэхенвжьфжпсхгчплвжмвиртдэппшуртцюиэппедчйдешорпдпвюбжлотвдюлофехщыдд
етеодайюяхрdbмлпнднелешхдошущазнибыутвднташебацэзьгордфесьаешзкнсднюятьд
аахмчвюцхеиовющежемпзькюжамюгьщцсбвдсчепзлепэшбмтвгоэвубюзмвппцинэзьэштапуи
эпхлеоенщнщрдэшлабмхтфуиюййаешэдэвлюцрпбжэщыдидсдщохилпийшгмищцвюбйощйапедм
лестгцатьчшбуэьгйцамиизавдкюяцрорпбдкьйомьщеаохдяючвейчвэухвьхэерючежюшзюахмр
пййзхфйдыжецэзчяшктьмоодььепюййайрюошюцдиена тшхщнеэмьхгьощеююиьвдгивюьжшухе
хшкдэшжюяцлшлейдюйбпгьюйййгдидндидбосдьдиараощаагюывмтвдцэзэяхщаййжтгпюфпэшя
иййхмлпияюцмахщмайвкмшувывбочвгййобуизывзджююцгйбасдйэвюэасуяхуцбушфлпэь
вмхшоеяхрпдюцибофебаитвлпхлпэьуеююэзлпбийэлпбинюфугьвоцвхестюцгдтэфйнезатшщ
авытдщааошумюжячаеаеаоодзтлояййысьюцсьмашайыьхлеяюсбфеюэшуйзлепрдюикизольуц
обуйюгктнвэиюдэяхщагююцхенедефепэлпсайикияшбушзшзунтахаьыхдрпдэшчижеьюхиб
унюзьдесьюцаешфеюайвкмжгеэзчхаздхенехднвяшжесьвчаеяютвючсьцукммюфпэьхцхене
ешжпмюфгцвцвзщяшдыэжежуйэфгэзюайгышоднвкгшвиьвчлпэьяьхэжмьхиьбшйыфпжягьмат
щаефмлестгцадьтцэьакгдйпгцэьдемимозщчртшгдцэьшщузмонпамвикнсшувлонвиюовкмле
бпчвмвзьжемвшзгдяиампнлоппбообхдвхшнвшуялнюгьэабуохобхдзечадыегжеышхдктеаю
аирюунедмшчуудвайыэанвфупдэмчвмьщелеяймоюааачвэуопэьжеюэюаееыпхщаазяхзснгые
тепюхизьаелецуктпмзшршеьбюекгдьвтшщдчиубждгдхецкнвюиэвднвфузчшщдетадшимжйц
умюэщйюшйаэмтщвдеьйомюхебавахивлфеионвздоубтесаыдхшнвшуцуюэрдцзшхмвлоцушц
шайюшдрддебочишукмжйпиуцфйжпшцоеидфгшйошемлмжгвдфвюаюобюаюьймвшжеэуяххарин
дшщэщгщчикгялнювамжфуошпйццмюегнщеегбдфюфпюйбпгьфпжйиэцвтбнщеегбмлешщзэяй
ьддьяецыфгсцфжтбшвяцвиошиалешщнвбчрийахиюючпммьшгяошулобжфгфиьжпптбшвиьийраы
ьнщчаощэшулопдишщцааявяцбуиьэшхдвыбшпееыаебухтвдсдошийшщцыэщзщцймилмлежшощ
растиаэиюшщййзащеоюиьцвмтшзлебджовшшхщужуиубэшулопдхомццвяйощвыявжявщэадо
щыштшкшфйыьжеуцшуднвлешэяхщабммоппмвппдюлмледшйидужижиженввииятпнзетечютд
юйбпгьчизднвепфйзшиакунэшщфпызайтьхиэианвзшущиорпбдпюцижефвчвйэгцлпнющеца
еямтштазаощськммочизилпбоодэаьдааощчвошюшдийрднпцвдщнюиадежпизвиьхсшрдехшу
йэтфппрюфпюцпмлпияшцоугьцааюфпэьавдтшфеоешпхэбонношиафпжяфпцвчвжьфждэлолвя
ьчвдодэайайыжевыоененезаиаразевыбвжйцулмлепешдерйхакииэяхщагютврюфпэшиацаыв
вюсюлоэуцвшэщйыаегюфпгьпднеизяшсджпннхезефюфпашчвэвьхлммьдшоюьхиьрйрарежюг
ьщелекштьээмюфзнэцвсдмааеюиэисьмюцвэиубэфгшдешечйшвзкоусжээштеяииюфггшкею
ччэацапесьзецуюмозьхцоуюеуюмодшаййыхетеуиэижецэзчтэгчййыбозэгчййымааейшгюд
пюйбпгьишшхйэзьлвепцвсдчйыутвывяцбехдыиьхзавдссяобамшсдэанелезатэфйфшиээшне
жетштгдидчвяроеуюжйжпннтвшивлугцхлехштапэсбеелеяоодгджубвюцдеюччшупнлмлеяеш
айыиалимьяшфгмючехйуышзкоусбшмазшбиьхзэзьйысьзьюауйжекюжмтшкдцьшхйэашцааюцв
мабзнэщегеюсюбжовшщцапейцшцвюлозьйычвийзаятдпэшьхлеяюсбеужищеегдьдэбоодфее
аоененетшкервтвэйтшчанезчудйожецэзчкмючсджэзлрдяюнюиюэзмюсетпыжташенепхсшыш
ьвчвнюлоизяцсбэапепешдийогдйыхедетамайвднвюдэяхщавооодбпртгьоецуппиачпковфн
дхшоедесшсдкюэьдэяцсдцааюцвэшфепэюцзасеяинэшзчуртэшсззеысдкюмвежцищемарцэл

утробы лотихоегорода ку танный ть мой мир не жил ся в постели пришло лето и ветер был летний теплоедыхание мира неспешное и ленивое стоить лишь встать высунуть ся во кошко и тотчас

поймешь вот она начинается с тобою и жизнь в то первое утро лета дуглас по динг двенадцати летотрол до тольк что открыл глаза и как в теплу речку погрузился в предрассветную безмятежность он лежал в сводчатой комнате на четвертом этаже во всем городе не было башни выше и от того что он парил так высоко в воздухе вместе сиюньским ветром в нем ожидалась чудодейственная сила по ночам когда вязы дубы и клены сливались в одно беспокойное море дуглас кидал вале говзглядом пронзавшим тьму точно маяк сегодня вот здорово спнул он впереди целое лето не считая множества в ней чуть неполка календаря он уже видел себя много раз как божество и в аиз книжки про путешествия тольк о попевай рвать еще зеленые яблоки персики черные как ночь сливы егоне вытащить из лесу изкустов из речки а как приятно будет померзнуть забравшись в заинде вельий ледник как весело жариться в бабушкиной кухне за одностысячью цыплят а пока задело раз в неделю ему позволяли ночевать в домике по соседству где спали его родители и младший братишка тома здесь в дедовской башне он в бегах по темной винтовой лестнице на самый верх и ложился спать в этой обители кудесника среди грома видений а спозаранку когда даже молоко не ели не звякала бутылка на улице он просыпался и приступал к заветному волшебству стоя в темноте у открытого окна он набрал полную грудь воздуха и из всех сил дунул уличные фонари мигнули погасли точно свечки на черном фоне неинно мирогедуглас дунул еще и еще и в небеначали гаснуть звезды дуглас улынулся ткнул пальцем там там теперь тут тут вот тут тут в предутреннем тумане один за другим прорезались прямо угольники в домах зажигались огни далеко далеко на рассветной земле в другом зарилась целая вереница окон в семзевнутрь в сем вставать огромный дом внизу ожил дедушка вынимай зубы из стакана дуглас немного подождет бабушка и прабабушка жарят оладьи сквозняк проронес по всем коридорам теплый дух жареного теста и во всех комнатах встали и пошевелились многочисленные тетки дяди двоюродные братья и сестры ч то с ехались сюда погостить улица стариков просыпайся мисс элен мисполковник фрилей миссис бенгли покашливает встань тепроглотите свои таблетки пошевеливайтесь мистер джон ас запрягайте лошадей выводите из сараи фургон пора ехать за старьем по ту сторону у врага открылись свои драконы и глаза угрюмые собняки скоровнизу появляются на электрической зеленой машине две старухи и покатят поутренним улицам приветственнао а каждая в своей встречной собаке мистер тридден бежит в трамвайное депо и в скором поезде ким ру сламощеныхулиц поплывет трамвай рассыпая вокруг жаркие искры джон хафчарливуд мены готовы еще поул дугласулице детей готовы спросить о побейсбольных мячах что мокли на росистых лужайках у пустых веревочных качелей что скучая свисали с деревьев в мам паптом проснитесь тихонько прозвенели будильники гулко побили часы на здании и судачно сесть заброшенная горойкой с деревьев ввзметнулись птицы иза пели дирижируя своим оркестром дуглас повелительно протянул руку к востоку и взошло солнце дуглас скрестил руки на груди и улынулся как настоящий волшебник вот то думал он тольк оя приказали все по в скали все забегали отличное будет лето и она на последок глядел гор одишелкнул ему пальцами и распахнулись двери домов людывышли на улицу летотысяча девятьсот двадцать восьмого года началось в утро проходя полужайке дуглас наткнулся на паутину невидимая нить коснулась его голба и не слышно опнула и оттого попустячного случая она сторожилась день будет не такой как в сене такой еще и потому что бываю т дни сотканые из одних запахов словно весь мир можно втянуть носом как воздух вдохнуть и выдохнуть так обяснял дугласу ие год десятилетнем у брату тому отец когда вез их в машину за город а в другие дни гворилеще отец можно услышать каждый громикаждый шорох в селеной иныедних хорошо пробовать на вкус аины на ощупь а бываю т такие когда ешь все сразу вот например сегодня пахнет такбудто в одну ночь там захолма мине весть откуда взялся огромный фруктовый сад в седосамо го горизонта так и благоухает в воздухе пахнет дождем но на небени облачка того и гляди кто неведомый захочет в лесу покатать мишина дуглас во все глаза смотрел на плывущие мимо поля не тинаса дом не пахнет ни дождем да и откуда бы разня яблоны не тнитучик то там может хохотать в лесу авсетаки дуглас вздрогнул деньэтот какой то особенный машина остановилась в самом сердце тихого леса а ну ребята не баловаться яони подталкивали друг друга локтями хорошо папа мальчики вылезли из машины захватили синеи жестяные ведра и сойдя спустынной проселочной дороге погрузились в запах земли влажной от недавнего дождя и тепчел сказал отец они в сегда вьются в возле винограда как мальчишки в возле кухни дуглас дуглас встали и поплываешь в облаках сказал отец спустись на землю пойдем с нами хорошо

апаиникусъкомбребилепесувпередитотещрослыйиплечистыйзанималдугласапоследним
семенилкоротышка томподнялисьнаневысокийхолмипосмотреливдальвонтамуказалпаль
цемотецтамобитаютогромныеполетнемутихиеветрыинезримыеплывутвзеленыхглубинах
точнопризрачныекитыдугластглянулвтусторонуничегонеувиделипочувствовалсебяобм
анутымотецкакидедушкавечноговоритзагадкамиииивсетакидугласзатаилдыханиеиприс
лушалсячтотодолжнослучитьсяподумалоняужзнаюавотпапоротникназываетсявенерин
олосотецнеторопливошагалвпередсинееведропозвякивалоунеговрुкеазточувствует
ионковырнулземлюноскомбашмакамиллионылеткопилсяэтотперегнойосеньзаосеньюпад
алилистьяпоказемлянесталатакоймягкойухтыяступаякакиндеецсказалтомсовсемнесл
ышнодугласпотрогалземлюноничегонеошутилонвсевремянастороженноприслушивалсям
ыокруженыдумалончтотослучитсяночтооностановилсывыхождаетытамчтотытакоемы
сленнокричалонтомиотецшлидальшепотихойподатливойземленасветенеткружеватоньш
енегромкосказалотеципоказалрукойвверхгделиствадеревьеввплеталасьвнебоилимож
етбытьнебовплеталосьвлиствувсеравноулыбнулсяотецвсезтокружевазеленыеиголубы
евсмотритехорошенькоиувидителесплететихсловногудящийстанокотецстоялуверен
нопохозяйскиирассказывалимвсякуювсичинулегкоисвободноневыбираясловчастоонис
амсмеялсясвоимрассказамиотэтогоонитеклиещесвободнеехорошоприслушаепослушать
тишинуговорилонпотомучтотогдадаетсяуслышатькакноситсяввоздухепыльцаполевых
цветолавоздухтакигудитпчеламидадатакигудитавотслышитетамзадеревьямиводопада
мльетсяптичьещебетаньевогсейчасдумалдугласвотонужеблизкоаяещеневижусовсемб
лизкорядомдикийвиноградсказалотецнамповезлосмотритеканенадоахнулпросебядугл
аснотомииотецнаклонилисьипогрузилирукившуршащийкустчарырассеялисьтопугающееи
грозноечтоподкрадывалосьблизилосьготовобылоринутьсяипотрястиегодушуисчезлоо
пустошенныйрастерянныйдугласупалнаколенипальцыегоушлиглубоковзеленуютенъивы
нырнулиоблагренныеалымсокомсловноонврезаллесножомисунулрукивоткрытуюранумал
ьчикизавтракатьведрачутьнедоверхунаполненыдикиимвиноградомилеснойземляникойв
округгудятпчелызэтововсенепчелыцелыймиртихонькомурлычетсвоюпесенкуговоритот
ецаонисидятназамшеломстволеупавшегодереважуютсандвичиипытаютсяслушатьлескак
слушаефонотецчутьпосмеиваясьискосапоглядываетнадугласахотелбылочтотосказать
нопромолчалоткусилещекусоксандвичаизадумалсяхлебсветчинойвлесунетчтодомавк
уссовсемдругойверноостреечтолимятойотдаетсмолойаужаппетиткакразыгрываетсяду
гласпересталжеватьипотрогалязыкомхлебиветчинунетнетобыкновенныйсандвичтомки
внулпродолжаяжеватьяпонимаюпапведьужепочтислучилосьдумаетдугласнезнаючтоэто
нонообольщущеепрямогромдаоечтотоегоспугнулогдежеонотеперьопятьушловтоткуст
нетгдетозамнойнетнетздесьтутрядомдугласисподтишкапощупалсвойживотоноещеверн
етсянадотольконемножкоподождатьбольнонебудетяужзнаюнезатемонокомнепридетноз
ачемжезачема

Висновки: в ході лабораторної роботи дослідили та реалізували метод розшифрування шифру афінної підстановки біграм. А також дізналися про критерії відбору змістовних текстів і реалізували один з них.